Integer Feasibility of Random Polytopes

Karthekeyan Chandrasekaran*
School of Engineering and Applied Sciences
Harvard University
karthe@seas.harvard.edu

Santosh S. Vempala†
School of Computer Science
Georgia Institute of Technology
vempala@gatech.edu

ABSTRACT

We study the Chance-Constrained Integer Feasibility Problem, where the goal is to determine whether the random polytope

$$P(A,b) = \{x \in \mathbb{R}^n : A_i x \leq b_i, i \in [m]\}$$

obtained by choosing the constraint matrix A and vector b from a known distribution is integer feasible with probability at least $1-\epsilon$. We consider the case when the entries of the constraint matrix A are i.i.d. Gaussian (equivalently are i.i.d. from any spherically symmetric distribution). The radius of the largest inscribed ball is closely related to the existence of integer points in the polytope. We find that for m up to $2^{O(\sqrt{n})}$ constraints (rows of A), there exist constants $c_0 < c_1$ such that with high probability ($\epsilon = 1/\text{poly}(n)$), random polytopes are integer feasible if the radius of the largest ball contained in the polytope is at least $c_1\sqrt{\log(m/n)}$; and integer infeasible if the largest ball contained in the polytope is centered at $(1/2,\ldots,1/2)$ and has radius at most $c_0\sqrt{\log(m/n)}$. Thus, random polytopes transition from having no integer points to being integer feasible within a constant factor increase in the radius of the largest inscribed ball. Integer feasibility is based on a randomized polynomial-time algorithm for finding an integer point in the polytope.

Our main tool is a simple new connection between integer feasibility and linear discrepancy. We extend a recent algorithm for finding low-discrepancy solutions to give a constructive upper bound on the linear discrepancy of random Gaussian matrices. By our connection between discrepancy and integer feasibility, this upper bound on linear discrepancy translates to the radius bound that guarantees integer feasibility of random polytopes.

*This work was done while the author was a student at Georgia Institute of Technology supported in part by the Algorithms and Randomness Center (ARC) fellowship and the NSF.
†Supported in part by NSF Award CCF-1217793.

ITCS'14, January 12–14, 2014, Princeton, New Jersey, USA.

http://dx.doi.org/10.1145/2554797.2554838.

Categories and Subject Descriptors

G.1.6 [**Optimization**]: Integer Programming; G.2.1 [**Discrete Mathematics**]: Combinatorics

General Terms

Theory, Algorithms

Keywords

Integer Programming, Probabilistic Instances, Discrepancy, Chance-Constrained Programs, Random Matrices

1. INTRODUCTION

Integer Linear Programming (IP) is a general and powerful formulation for combinatorial problems [29, 23]. One standard variant is the integer feasibility problem: given a polytope $P \in \mathbb{R}^n$ specified by linear constraints $Ax \leq b$, find an integer solution in P or report that none exists. The problem is NP-hard and appears in Karp's original list [15]. Dantzig [10] suggested the possibility of IP being a *complete* problem even before the Cook-Levin theory of NP-completeness. The best-known rigorous bound on the complexity of general IP is essentially $n^{O(n)}$ from 1987 [14] with only small improvements in the constant in the exponent since then [13, 9].

While IP in its general form is intractable, several special instances are very interesting and not yet well-understood. One such simple and natural family of instances is randomly generated IP instances, where the constraints describing random polytopes are drawn from a distribution. The class of optimization problems defined by such probabilistic constraints is known as Chance-Constrained Programming in Operations Research and their continuous optimization versions have been well-studied [7, 22, 26]. In its general form, a Chance-Constrained Linear Program (CCLP) with a joint probabilistic constraint is given by: $\max\{c^T x : A'x \leq b', \mathsf{Pr}(Ax \leq b) \geq 1-\epsilon\}$ for some chosen confidence parameter ϵ as required in the application. Here the probability is over the random choice of (A,b). CCLPs are powerful in modeling uncertainty in the availability of the resources and have found applications in supply chain management, circuit manufacturing, energy production, telecommunications, etc. [26, 27].

In this paper, we address the Chance-Constrained Integer Feasibility problem, where the goal is to determine whether the random polytope $\{x : Ax \leq b\}$ obtained by choosing A and b from a known distribution is integer feasible with probability at least $1-\epsilon$, We assume the constraint matrix

A is chosen randomly while the choice of b is deterministic, and ϵ is taken to be inverse polynomial in the dimension.

Random instances have been studied for several combinatorial problems e.g., random-SAT [4, 5, 8, 3, 11], random knapsack [1], and various other graph problems on random graphs [2]. Chance-constrained subset-sum IP was first studied by Furst and Kannan [12]. Their results were generalized to multi-row IP by Pataki et al. [25]. They showed that if each entry in the constraint matrix A is chosen independently and uniformly at random from the discrete set $\{1, 2, \ldots, M\}$, then with high probability, a certain reformulation of such random IP instances can be solved efficiently by the branch-and-bound algorithm provided that M is sufficiently large. These and other models for chance-constrained programs [28, 19, 18, 32] address the finite-case scenario in which the number of possible outcomes of (A, b) is finite. In contrast, here we addresse the continuous scenario.

Model for random IPs. A random IP instance in our model is described by a random constraint matrix $A \in \mathbb{R}^{m\times n}$ and an RHS vector b. Formally, we obtain random IP instances by generating random polytopes $P(n, m, x_0, R) = \{x \in \mathbb{R}^n : A_i x \leq b_i \ \forall\ i \in [m]\}$ as follows: pick a random $m \times n$ matrix A with i.i.d. entries from the Gaussian distribution $N(0, 1)$; and a vector b such that the hyperplane corresponding to each constraint is at distance at least R from x_0, i.e., denoting the i'th row of A as A_i,

$$\frac{b_i - A_i x_0}{\|A_i\|} \geq R$$

or

$$b_i \geq A_i x_0 + R\|A_i\|.$$

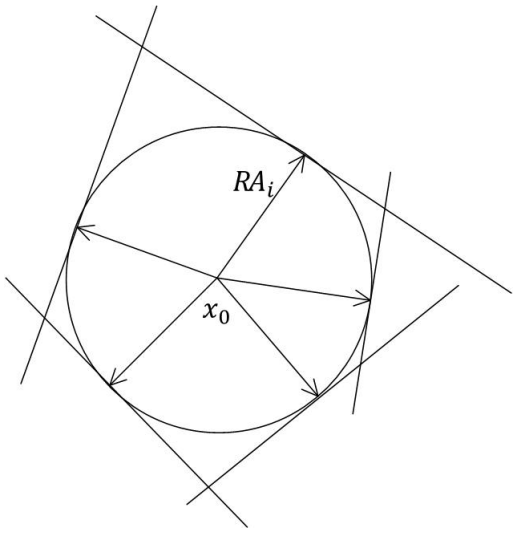

Figure 1: A Random IP instance $P(n, m, x_0, R)$ with facet normals being random unit vectors A_i and each facet at distance at least R from x_0.

An equivalent geometric interpretation for our model of random polytopes is the following (see Figure 1): we recall that if each row of the constraint matrix A is a unit vector, then they describe the normals to the facets of the polytope $P = \{x : Ax \leq b\}$. Thus, the random polytopes $P(n, m, x_0, R)$ in our model are obtained using m facets whose normal vectors are independent uniform random unit vectors in $\mathbb{R}^n$ and such that each facet is at distance R from the point x_0.

The condition that all facets are at distance at least R from x_0 is equivalent to the condition that $P(n, m, x_0, R)$ contains a ball of radius R centered at x_0. We study the integer feasibility of $P(n, m, x_0, R)$ for every x_0 as a function of the radius R. As R increases, intuitively it is more likely that the polytope contains an integer point.

Contributions. We show a phase-transition phenomenon regarding integer feasibility of random polytopes with respect to the radius used to generate these polytopes — we show an upper bound on R needed to guarantee integer feasibility with high probability for every $x_0 \in \mathbb{R}^n$; we show a lower bound that guarantees integer infeasibility with high probability for a fixed $x_0 = (1/2, \ldots, 1/2)$; our upper and lower bounds differ by a constant factor when m is at most $2^{O(\sqrt{n})}$. We show our upper bound via an efficient algorithm to find an integer feasible solution in the feasibility regime. This is an application of a recent constructive proof in discrepancy theory [17].

Alternatively, our results can be reinterpreted to bear resemblance to the well-known random SAT threshold: consider random polytopes in n-dimensions obtained by picking m random tangential hyperplanes to a ball of "constant" radius centered at x_0. If $m \leq c_0 n$, then random polytopes are integer feasible for every x_0 with high probability and if $m \geq c_1 n$, then random polytopes are integer infeasible for $x_0 = (1/2, \ldots, 1/2)$. Thus, integer feasibility of random polytopes exhibits a phase transition-like behavior when the number of hyperplanes increases beyond a constant times the number of variables, closely resembling the behaviour of random k-SAT.

Our main conceptual (and simple) contribution is a new sufficient condition to guarantee integer feasibility of *arbitrary* polytopes. The idea is that a polytope is likely to contain an integer point if it contains a large ball. In fact, any polytope in n-dimensional space that contains a Euclidean ball of radius at least $\sqrt{n}/2$ is integer feasible. We refine this radius $r(A)$ of the largest inscribed ball that guarantees integer feasibility as a function of the constraint matrix A describing the polytope. This refined radius function is helpful in deriving bounds on the radius of the largest inscribed ball that guarantees integer feasibility of random polytopes.

For $R = \Omega(\sqrt{\log m})$ and $x_0 = (1/2, ...1/2)$, there is a trivial algorithm: pick a random 0/1 vector. Most such vectors will be feasible in $P(n, m, x_0, R)$. But with smaller R, and arbitrary centers x_0, only an exponentially small fraction of nearby integer vectors might be feasible, so such direct sampling/enumeration would not give a feasible integer point. We use a more careful sampling technique for smaller R. As mentioned earlier, this is a straightforward extension of a recent algorithm for finding low discrepancy solutions [17].

1.1 Results

Our main theorem is stated as follows.

THEOREM 1. *Let* $1000n \leq m \leq 2^n$ *and*

$$R_0 = \sqrt{\frac{1}{6}\log\frac{m}{n}},$$

$$R_1 = 384\left(\sqrt{\log\frac{m}{n}} + \sqrt{\frac{\log m \log(mn)\log(m/\log m)}{n}}\right).$$

Then,

1. *there exists a randomized polynomial time algorithm that with probability at least* $1-(4/m^3)-2me^{-n}$ *finds an integer point in the random polytope* $P(n,m,x_0,R)$ *for any* $x_0 \in \mathbb{R}^n$ *and* $R \geq R_1$,

2. *with probability at least* $1-2^{-n}-2me^{-n}$, *the random polytope* $P(n,m,x_0=(1/2,\ldots,1/2),R)$ *does not contain an integer point if* $R \leq R_0$.

We remark that these results continue to hold in the equivalent random polytope model $P(n,m,x_0,R)$ obtained using random matrices A whose rows are chosen i.i.d. from any spherically symmetric distribution.

Remarks.

1. For $m = 2^{O(\sqrt{n})}$, the second term in R_1 is of the same order as the first and so R_0 and R_1 are within a constant factor of each other. Thus, in this case, the transition between infeasibility and feasibility happens within a constant factor increase in the radius.

2. When $m = cn$ for some sufficiently large constant c, our theorem shows that a constant radius ball inscribed in random polytopes is sufficient to guarantee integer feasibility with high probability (as opposed to the $\sqrt{n}/2$ radius ball needed in the case of arbitrary polytopes).

Underlying the above theorem is a simple yet powerful connection between the radius of the largest inscribed ball that guarantees integer feasibility and the linear discrepancy of the constraint matrix. If the radius is at least the linear discrepancy of the normalized constraint matrix (each row is normalized to a unit vector), then the polytope contains an integer point.

The linear discrepancy of a matrix $A \in \mathbb{R}^{m\times n}$ is defined as follows [20, 30, 31]:

$$\text{lin-disc}(A) := \max_{x_0\in[0,1]^n} \min_{x\in\{0,1\}^n} \|A(x-x_0)\|_\infty .$$

PROPOSITION 1. *Every polytope*

$$P_{x_0}(A) = \{x \in \mathbb{R}^n \,|\, |A_i(x-x_0)| \leq b_i \text{ for } i \in [m]\}$$

where $b_i \geq$ *lin-disc*(A) *contains an integer point for any* $x_0 \in \mathbb{R}^n$.

We elaborate on Proposition 1 in Section 1.2. To apply this connection to random IPs, we bound the linear discrepancy of Gaussian matrices.

THEOREM 2. *Let* $A \in \mathbb{R}^{m\times n}$ *be a random matrix with i.i.d. entries from* $N(0,\sigma^2)$, *where* $2n \leq m \leq 2^n$. *There exists an algorithm that takes a point* $x_0 \in \mathbb{R}^n$ *as input and outputs a point* $x \in \mathbb{Z}^n$ *by rounding each coordinate of* x_0 *either up or down such that, for every* $i \in [m]$,

$$|A_i(x-x_0)| \leq 192\sigma\left(\sqrt{n\log\frac{m}{n}} + \sqrt{\log m\log(mn)\log\frac{m}{\log m}}\right).$$

with probability at least $1-(4/m^3)$. *Moreover, the algorithm runs in expected time that is polynomial in* n *and* m.

In terms of classical discrepancy theory, Theorem 2 is equivalent to a bound of $O(\sigma R_1\sqrt{n})$ on the linear discrepancy of random Gaussian matrices. The integer feasibility in Theorem 1 (part 1) follows from Theorem 2 by choosing $\sigma^2 = 1$ and observing that with probability at least $1-2me^{-n}$, all m random Gaussian vectors in n-dimension have length $O(\sqrt{n})$.

1.2 The Discrepancy Connection

To understand this connection, we begin with a simpler problem where $x_0 = 0$ and our goal is to find a point in the polytope with all coordinates in $\{-1,1\}$ (as opposed to integer points). Given a matrix $A \in \mathbb{R}^{m\times n}$, and a real positive value r, consider the polytope $P(A,r) = \{x \in \mathbb{R}^n : |A_i x| \leq r \;\forall\; i \in [m]\}$. The discrepancy of a matrix A is defined to be the least r so that the polytope $P(A,r)$ contains a $-1/1$ point. This is equivalent to the classical definition of discrepancy [20, 30, 31]:

$$\text{disc}(A) := \min_{x\in\{-1,+1\}^n} \|Ax\|_\infty .$$

The following proposition is an immediate consequence of this definition.

PROPOSITION 2. *The polytope* $P(A, \text{disc}(A)) = \{x \in \mathbb{R}^n : |A_i x| \leq \text{disc}(A) \;\forall\; i \in [m]\}$ *contains a point with all* $-1/1$ *coordinates.*

To see this, observe that the point $x \in \{-1,+1\}^n$ that minimizes discrepancy is in fact contained in the polytope $P(A, \text{disc}(A))$. Thus, if we can evaluate the discrepancy of the constraint matrix A, then by verifying whether the infinity norm of the RHS vector is at least $\text{disc}(A)$, we have an easy heuristic to verify if the polytope contains a $-1/1$ point. Hence, if each row of A is a normalized unit vector, then the polytope $Ax \leq b$ contains a $-1/1$ point if it contains a ball of radius at least $\text{disc}(A)$ centered at the origin.

The related notion of linear discrepancy helps in providing a sufficient condition for *integer feasibility* (as opposed to $-1/1$ feasibility) of arbitrary polytopes. Proposition 1, similar to Proposition 2, is an immediate consequence of the definition of linear discrepancy. This is because, by linear transformation, we may assume that x_0 is in the fundamental cube defined by the standard basis unit vectors. Thus, if each row of the matrix $A \in \mathbb{R}^{m\times n}$ is a unit vector, then the linear discrepancy of the constraint matrix gives a radius for the largest inscribed ball that guarantees integer feasibility of polytopes described by the constraint matrix A.

The approach suggested by Proposition 1 to verify integer feasibility of arbitrary polytopes requires the computation of linear discrepancy of arbitrary matrices. The related problem of computing the discrepancy of arbitrary matrices even to within an approximation factor of $\sqrt{n}$ is known to be NP-hard [6]. In recent work, Nikolov, Talwar and Zhang [24]

have shown that *hereditary discrepancy*, which is an upper bound on linear discrepancy (see Theorem 4 below), can be efficiently computed to within an approximation factor of $poly(\log m, \log n)$; this could potentially be useful as a heuristic to verify integer feasibility (approximately).

In order to understand the integer feasibility of random polytopes using this approach, we seek a bound on the linear discrepancy of random matrices that holds with high probability. We obtain such a tight bound for random matrices algorithmically by extending a recent constructive algorithm that minimizes discrepancy [17] to an algorithm that minimizes *linear* discrepancy. Our infeasibility threshold is also based on discrepancy — we begin with a lower bound on the discrepancy of random matrices, which excludes any 0/1 point from being a feasible solution for $P(n, m, x_0 = (1/2, \ldots, 1/2), R_0)$, and then extend this to exclude all integer points.

2. PRELIMINARIES

2.1 Related Work

The central quantity that leads to all known bounds on discrepancy and linear discrepancy in the literature is hereditary discrepancy defined as follows:

$$\text{herdisc}(A) := \max_{S \subseteq [n]} \text{disc}(A^S)$$

where A^S denotes the submatrix of A containing columns indexed by the set S. For a matrix $A \in \mathbb{R}^{m \times n}$ and any $S \subseteq [n]$, let ${A_i}^S$ denote the i'th row vector A_i restricted to the coordinates in S. The best known bound on discrepancy of arbitrary matrices is due to Spencer [30].

THEOREM 3. *[30] For any matrix $A \in \mathbb{R}^{m \times n}$, any subset $S \subseteq [n]$, there exists a point $z \in \{-1, +1\}^{|S|}$ such that for every $i \in [m]$,*

$$\left|{A_i}^S z\right| \leq 11\sqrt{|S| \log \frac{2m}{|S|}} \max_{k \in [m],\ j \in S} |A_{kj}|.$$

Lovász, Spencer and Vesztergombi [16] showed the following relation between hereditary discrepancy and linear discrepancy.

THEOREM 4. *[16] For any matrix A,*

$$\textit{lindisc}(A) \leq \textit{herdisc}(A).$$

2.2 Concentration Inequalities

We will use the following well-known tail bounds.

LEMMA 3. *Let Y be a random variable drawn from the Gaussian distribution $N(0, \sigma^2)$. For any $\lambda > 0$,*

$$\mathsf{Pr}\left(Y \leq \lambda\sigma\right) \leq \min\left\{1 - \sqrt{\frac{1}{2\pi}}\left(\frac{\lambda}{\lambda^2+1}\right)e^{-\frac{\lambda^2}{2}}, \lambda\sqrt{\frac{1}{2\pi}}\right\}.$$

LEMMA 4. *Let Y be a random variable drawn from the Gaussian distribution $N(0, \sigma^2)$. For any $\lambda \geq 1$,*

$$\mathsf{Pr}\left(|X| \geq \lambda\sigma\right) \leq 2e^{-\frac{\lambda^2}{4}}.$$

LEMMA 5. *Let $X_1, \ldots, X_n$ be independent random variables each drawn from the Gaussian distribution $N(0, \sigma^2)$. For any $\lambda \geq 1$,*

$$\mathsf{Pr}\left(|\sum_{j \in [n]} X_j^2 - n\sigma^2| \geq c\lambda\sqrt{n}\sigma^2\right) \leq 2e^{-\lambda^2}$$

for an absolute constant c.

LEMMA 6. *[21] Let $X_1, \ldots, X_n$ be independent random variables each drawn uniformly from $\{-1, +1\}$. For a fixed set of vectors $a_1, \ldots, a_m \in \mathbb{R}^n$, a fixed subset $S \subseteq [n]$, and any $\lambda \geq 0$,*

$$\mathsf{Pr}\left(|\sum_{j \in S} a_{ij} X_j| \geq \lambda\right) \leq 2e^{-\frac{\lambda^2}{2\sum_{j \in S} a_{ij}^2}}.$$

3. LINEAR DISCREPANCY OF RANDOM MATRICES

Our first step towards an algorithm to identify an integer point in random polytopes is an algorithm to find small linear discrepancy solutions for random Gaussian matrices. The main goal of this section is to prove the bound on linear discrepancy of Gaussian matrices (Theorem 2).

Implications of known bounds. It is tempting to use known concentration inequalities in conjunction with Spencer's result (Theorem 3) to bound the hereditary discrepancy of Gaussian matrices; this would in turn lead to a bound on the linear discrepancy of Gaussian matrices by Theorem 4. In this setting, each entry A_{ij} is from $N(0, \sigma^2)$. Using standard concentration for $|A_{ij}|$ and a union bound to bound the maximum entry $|A_{ij}|$ leads to the following weak bound: with high probability, the polytope $P = \{x \in \mathbb{R}^n \,|\, |A_i(x - x_0)| \leq b_i \text{ for } i \in [m]\}$ with $b_i = \Omega(\sigma\sqrt{n \log mn \log(2m/n)})$ contains an integer point for any $x_0 \in \mathbb{R}^n$. This is too weak for our purpose (recall that $\sqrt{n}$ radius ball in arbitrary polytopes already guarantees integer feasibility and our goal is to guarantee integer feasibility with smaller inscribed ball in *random* polytopes).

Our Strategy. Our overall strategy to bound discrepancy is similar to that of Spencer's: As a first step, show a partial coloring with low discrepancy – i.e., for any subset $U \subseteq [n]$, there exists a point $z \in \{0, -1, +1\}^{|U|}$ with at least $|U|/2$ non-zero coordinates such that $|A_i^U z|$ is small. Next for any $S \subseteq [n]$, repeatedly use the existence of this partial vector to derive a vector $x \in \{-1, 1\}^{|S|}$ with small discrepancy – start with $x = 0$, $U = S$ and use z to fix at least half of the coordinates of x to $+1$ or -1; then take U to be the set of coordinates that are set to zero in the current x and use z to fix at least half of the remaining coordinates of x to $+1$ or -1; repeat this until all coordinates of x are non-zero. Since at most $|U|/2$ coordinates are set to zero in each round of fixing coordinates, this might repeat at most $\log|S| \leq \log n$ times. The total discrepancy is bounded by the sum of the discrepancies incurred in each round of fixing. Thus, the goal is to bound the discrepancy incurred in each partial coloring round.

The discrepancy incurred for the i'th constraint by the partial coloring can be bounded as follows[1]:

$$|A_i{}^U z| \leq 4\,\|A_i{}^U\| \sqrt{\log \frac{2m}{|U|}} \quad \forall\, i \in [m],\ U \subseteq [n]. \qquad (1)$$

Bounding discrepancy of partial vector. The discrepancy bound for the i'th constraint given in (1) depends on the length of the vector $A_i{}^U$. We describe a straightforward approach that does not lead to tight bounds.

Approach 1. It is straightforward to obtain $\|A_i{}^U\| \leq 2\sigma\sqrt{|U|\log mn}$ with high probability for random Gaussian vectors A_i using well-known upper bound on the maximum coefficient of $A_i{}^U$. This leads to an upper bound of

$$8\sigma\sqrt{|S|\log(mn)\log\frac{2m}{|S|}}$$

on the discrepancy of A^S. Although this bound on the discrepancy of A^S is good enough when the cardinality of S is smaller than some threshold, it is too large for large sets S. E.g., when $S = [n]$, this gives a total discrepancy of at most $O(\sigma\sqrt{n\log(mn)\log(2m/n)})$.

New Approach. In order to obtain tighter bounds, we bound the length of partial vectors $A_i{}^U$ when each entry in the vector is from $N(0,\sigma^2)$ (as opposed to bounding the maximum coefficient). Using Lemma 5, we will show that

$$\|A_i{}^U\| = O\left(\sigma\sqrt{|U|}\left(\log\frac{en}{|U|}\right)^{\frac{1}{4}}\right)$$

for every $U \subseteq [n]$ of size larger than $\log m$ with probability at least $1 - 1/m^5$. Consequently, the total discrepancy incurred while the number of coordinates to be fixed is larger than $\log m$ is bounded by a geometric sum which is at most

$$O\left(\sigma\sqrt{n\log\frac{m}{n}}\right).$$

When the number of coordinates to be fixed is less than $\log m$, we use Approach 1 to bound the length of partial vectors, which in turn implies the required bound on the total discrepancy.

3.1 Bounding lengths of Gaussian subvectors

LEMMA 7. *Let $A \in \mathbb{R}^{m\times n}$ be a matrix whose entries are drawn i.i.d. from the Gaussian distribution $N(0,\sigma^2)$. Then, with probability at least $1 - 1/(mn)^3$,*

$$\|A_i{}^S\| \leq 2\sigma\sqrt{|S|\log mn}\ \forall S \subseteq [n],\ \forall i \in [m].$$

PROOF. By Lemma 4 and union bound over the choices of $i \in [m], j \in [n]$, all entries $|A_{ij}| \leq 2\sigma\sqrt{\log mn}$ with probability at least $1 - 1/(mn)^3$. Now, the squared length is at most the squared maximum entry multiplied by the number of coordinates. □

Next we obtain a bound on the length of $A_i{}^S$ when $|S|$ is large.

LEMMA 8. *Let $A \in \mathbb{R}^{m\times n}$ be a matrix whose entries are drawn i.i.d. from $N(0,\sigma^2)$ where $m \leq 2^n$. Then,*

$$Pr\,(\exists S \subseteq [n], |S| \geq \log m, \exists i \in [m] :$$
$$\|A_i{}^S\|^2 \geq 2\sigma^2|S|\sqrt{\log\left(\frac{en}{|S|}\right) + \frac{1}{|S|}\log m}\Bigg)$$
$$\leq \frac{1}{m^5}.$$

PROOF. Let

$$\lambda_s := 2\sqrt{s\log\left(\frac{en}{s}\right) + \log m}.$$

Fix a subset $S \subseteq [n]$ of size $|S| = s$ and $i \in [m]$. Then, by Lemma 5, we have that, for any $\lambda_s \geq 1$

$$\mathsf{Pr}\left(\|A_i{}^S\|^2 \geq s\sigma^2\left(1 + \frac{\lambda_s}{2\sqrt{s}}\right)\right) \leq 2e^{-\lambda_s^2}.$$

Hence,

$$\Pr\left(\exists S \subseteq [n], |S| = s, \exists i \in [m] : \|A_i{}^S\|^2 \geq s\sigma^2\left(1 + \frac{\lambda_s}{2\sqrt{s}}\right)\right)$$
$$\leq 2e^{-\lambda_s^2}\cdot\binom{n}{s}\cdot m \leq 2e^{-\lambda_s^2}\cdot\left(\frac{en}{s}\right)^s\cdot m$$
$$\leq 2e^{-\lambda_s^2 + s\log\frac{en}{s} + \log m} \leq 2e^{-3\left(s\log\frac{en}{s} + \log m\right)}.$$

Therefore,

$$\Pr\left(\exists S \subseteq [n], |S| \geq \log m, \exists i \in [m] : \|A_i{}^S\|^2 \geq |S|\sigma^2\left(1 + \frac{\lambda_{|S|}}{2\sqrt{|S|}}\right)\right)$$
$$= \Pr\left(\exists s \in \{\log m, \ldots, n\}, \exists S \subseteq [n], |S| = s, \exists i \in [m] : \|A_i{}^S\|^2 \geq s\sigma^2\left(1 + \frac{\lambda_s}{2\sqrt{s}}\right)\right)$$
$$\leq \sum_{s=\log m}^{n} 2e^{-3\left(s\log\frac{en}{s} + \log m\right)} = \left(\frac{2}{m^3}\right)\sum_{s=\log m}^{n} e^{-3s\log\frac{en}{s}}$$
$$\leq \left(\frac{2n}{m^3}\right)e^{-3\log m\log\frac{en}{\log m}} \leq \frac{1}{m^5}.$$

The last but one inequality is because the largest term in the sum is $e^{-3\log m\log(en/\log m)}$. The last inequality is because $n \geq \log m$.

Now, substituting for λ_s, we observe that

$$\sigma^2|S|\left(1 + \frac{\lambda_{|S|}}{2\sqrt{|S|}}\right) \leq 2\sigma^2|S|\sqrt{\log\left(\frac{en}{|S|}\right) + \frac{1}{|S|}\log m}.$$

□

[1]This is an improvement on the bound shown by Spencer: $|A_i{}^S z| = O\left(\max_{i\in[m],j\in S}|A_{ij}|\sqrt{|S|\log\frac{2m}{|S|}}\right)$ which can be recovered from (1). The proof of (1) is identical to the proof of Spencer's bound except for a stronger concentration inequality. We avoid the non-constructive proof for simplicity of presentation; we use an alternative algorithmic proof that follows from Lovett-Meka's partial coloring algorithm (see Lemma 9).

3.2 Algorithmic Linear Discrepancy

Our algorithm is essentially a variation of Lovett-Meka's algorithm for constructive discrepancy minimization [17]. Lovett-Meka [17] provide a constructive partial coloring algorithm matching Spencer's bounds. The main difference in their approach from that of Spencer's is that, the partial coloring algorithm outputs a fractional point $z \in [-1,1]^{|U|}$ such that at least $|U|/2$ coordinates are close to being 1 or -1. After at most $\log |S|$ rounds, all coordinates are close to being 1 or -1; a final randomized rounding step increases the total discrepancy incurred only by a small amount.

Their partial coloring algorithm can easily be extended to minimize linear discrepancy as opposed to discrepancy. In each partial coloring round, their algorithm starts with a point $x \in [-1,1]^n$ and performs a random walk to arrive at a vector y such that the discrepancy overhead incurred by y (i.e., $|A_i(y-x)|$) is small. Further, at least half of the coordinates of x that are far from 1 or -1 are close to 1 or -1 in y. This can be extended to an algorithm which, in each phase, starts with a point $x \in [0,1]^n$, and performs a random walk to arrive at a vector y such that the discrepancy overhead incurred by y (i.e., $|A_i(y-x)|$) is small. Further, at least half of the coordinates of x that are far from 0 or 1 are close to 0 or 1 in y. The functionality of such a partial coloring algorithm is summarized in the following lemma. In the rest of this section, given $x \in [0,1]^n$, $\delta \in \mathbb{R}$, let $B(x) := \{j \in [n] : \delta < x(j) < 1-\delta\}$.

LEMMA 9. *[17] Given $x \in [0,1]^n$, $\delta \in (0, 0.5]$, $A_1, \ldots, A_m \in \mathbb{R}^n$, $c_1, \ldots, c_m \geq 0$ such that $\sum_{i=1}^m exp(-c_i^2/16) \leq |B(x)|/16$, there exists a randomized algorithm which with probability at least 0.1 finds a point $y \in [0,1]^n$ such that*

1. $|A_i(y-x)| \leq c_i ||{A_i}^{B(x)}||_2 \ \forall\ i \in [m]$,
2. $|B(y)| \leq |B(x)|/2$
3. *If $j \in [n] \setminus B(x)$, then $y(j) = x(j)$.*

Moreover, the algorithm runs in time

$$O((m+n)^3 \delta^{-3} \log(nm/\delta)).$$

We denote the algorithm specified in Lemma 9 as Edge-Walk. To minimize the linear discrepancy of random Gaussian matrices, we repeatedly invoke the Edge-Walk algorithm. We repeat each invocation until it succeeds, so our algorithm is a Las Vegas algorithm. Each successful call reduces the number of coordinates that are far from being integer by at least a factor of $1/2$. Thus, we terminate in at most $\log n$ successful calls to the algorithm. Further, the total discrepancy overhead incurred by x is at most the sum of the discrepancy overhead incurred in each successful call. The sum of the discrepancy overheads will be bounded using Lemmas 7 and 8. Finally, we do a randomized rounding to obtain integer coordinates from near-integer coordinates. By standard Chernoff bound, the discrepancy incurred due to randomized rounding will be shown to be small.

PROOF OF THEOREM 2. Without loss of generality, we may assume that $x_0 \in [0,1]^n$ and our objective is to find $x \in \{0,1\}^n$ with low discrepancy overhead. We use Algorithm Round-IP given in Figure 1. We will show that, with probability at least $1 - 4/m^3$, it outputs a point $z \in \{0,1\}^n$

Algorithm 1 Algorithm Round-IP

Input: Point $x_0 \in \mathbb{R}^n$, matrix $A \in \mathbb{R}^{m \times n}$ where each $A_{ij} \sim N(0, \sigma^2)$.
Output: An integer point z.

1. Initialize. $x = x_0 - \lfloor x_0 \rfloor$, $\delta = 1/8 \log m$, $B(x) := \{j \in [n] : \delta < x(j) < 1-\delta\}$, $c_i = 8\sqrt{\log(m/|B(x)|)}$ for every $i \in [m]$.

2. While($|B(x)| > 0$)

(i) Edge-Walk. $y \leftarrow$ Edge-Walk(x, δ, $A_1, \ldots, A_m$, $c_1, \ldots, c_m$).

(ii) Verify and repeat. $B(y) := \{j \in [n] : \delta < y(j) < 1-\delta\}$. If $|B(y)| > |B(x)|/2$ or $|A_i(y-x)| > c_i ||{A_i}^{B(x)}||_2$ for some $i \in [m]$, then return to (i).

(iii) Update. $x \leftarrow y$, $B(x) = \{j \in [n] : \delta < x(j) < 1-\delta\}$, $c_i = 8\sqrt{\log(m/|B(x)|)}\ \forall\ i \in [m]$.

3. Randomized Rounding. For each $j \in [n]$ set

$$z(j) = \begin{cases} \lceil x_0(j) \rceil \text{ with probability } x(j), \\ \lfloor x_0(j) \rfloor \text{ with probability } 1 - x(j). \end{cases}$$

4. Output z.

such that

$$|A_i(z - x_0)| \leq 192\sigma \left(\sqrt{n \log \frac{m}{n}} + \sqrt{\log m \log(mn) \log \frac{m}{\log m}} \right).$$

Let $\overline{x}$ denote the vector at the end of Step 2 in Algorithm Round-IP and let x_k denote the vector x in Algorithm Round-IP after k successful calls to the Edge-Walk algorithm. By a successful call, we mean that the call passes the verification procedure 2(ii) without having to return to 2(i). Let $S_k = B(x_k)$. We first observe that after $k-1$ successful calls to the Edge-Walk subroutine, we have $\sum_{i=1}^m exp(-c_i^2/16) \leq |S_k|/16$ by the choice of c_is. By Lemma 9, the discrepancy overhead incurred in the k'th successful call to the Edge-Walk subroutine is

$$|A_i(x_k - x_{k-1})| \leq 8 \left\| {A_i}^{S_k} \right\| \sqrt{\log \frac{m}{|S_k|}}.$$

Consequently, the total discrepancy is bounded by the sum of the discrepancy overhead incurred in each run. The discrepancy overhead incurred in the k'th successful run, where $k : |S_k| \geq \log m$, is at most

$$8\sigma \sqrt{2|S_k| \log \frac{m}{|S_k|}} \left(\log \frac{en}{|S_k|} + \frac{1}{|S_k|} \log m \right)^{\frac{1}{4}} \leq 16\sigma \sqrt{|S_k| \log \frac{m}{|S_k|}} \left(\log \frac{en}{|S_k|} \right)^{\frac{1}{4}}$$

with probability at least $1 - (1/m^5)$. This is using the bound on the length of ${A_i}^{S_k}$ by Lemma 8.

Let k_1 be the largest integer such that $|S_{k_1}| > \log m$. Thus, with probability at least $1 - (1/m^5)$, the discrepancy overhead incurred after k_1 successful calls to the Edge-Walk

subroutine is at most

$$D_1 := 16\sigma \sum_{k=0}^{\log \frac{n}{\log m}} \sqrt{n2^{-k}\left(\log \frac{m}{n2^{-k}}\right)\sqrt{\log \frac{e}{2^{-k}}}} \leq 96\sigma\sqrt{n\log\frac{m}{n}}.$$

The upper bound on D_1 follows from the following inequalities (by setting $A = m/n$),

$$\sqrt{\left(\log \frac{A}{2^{-k}}\right)\sqrt{\log \frac{e}{2^{-k}}}} \leq \left(\sqrt{\log A} + \sqrt{k\log 2}\right)(1+k\log 2)^{\frac{1}{4}} \ \forall\ A \geq 1, \quad (2)$$

$$\sum_{k=0}^{\infty} \sqrt{2^{-k}(\log A)}\,(1+k\log 2)^{\frac{1}{4}} \leq 5\sqrt{\log A}, \quad (3)$$

$$\sum_{k=0}^{\infty} \sqrt{2^{-k}\cdot k\log 2}\,(1+k\log 2)^{\frac{1}{4}} \leq 2(\log 2)^{3/4}\sum_{k=0}^{\infty}\sqrt{2^{-k}}k^{3/4} \leq 10. \quad (4)$$

By Lemma 9, the discrepancy overhead incurred in the k'th successful call to the Edge-Walk subroutine, where $k : |S_k| \leq \log m$, is

$$|A_i(x_k - x_{k-1})| \leq 8\left\|A_i{}^{S_k}\right\|\sqrt{\log\frac{m}{|S_k|}} \leq 16\sigma\sqrt{n2^{-k}\log(mn)\log\frac{m}{n2^{-k}}}$$

with probability at least $1 - 1/(mn)^3$. Here, the second inequality is by using Lemma 7 and $|S_k| \leq n2^{-k}$. Since each successful call to the Edge-Walk subroutine reduces $B(x)$ by at least half, the number of successful Edge-Walk subroutine calls is at most $\log n$.

Thus, with probability at least $1 - 1/(mn)^3$, the discrepancy overhead incurred by Step 2 in successful rounds $k : |S_k| \leq \log m$ is at most

$$D_2 := \sum_{k=\log\frac{n}{\log m}}^{\log n} 16\sigma\sqrt{n2^{-k}\log(mn)\log\frac{m}{n2^{-k}}}$$

Now, using the inequalities (2), (3) and (4),

$$D_2 \leq 32\sigma\sqrt{\log m\log(mn)\log\frac{m}{\log m}}.$$

Hence, with probability at least $(1-1/m^5)(1-1/(mn)^3)$, at the end of Step 2, we obtain a point $\overline{x}$ such that $\overline{x} \in [0,1]^n$ and $\overline{x}(j) \geq 1-\delta$ or $\overline{x}(j) \leq \delta$ for every $j \in [n]$ and the total discrepancy overhead is bounded as follows:

$$\max_{i\in[m]}|A_i(\overline{x} - x_0)| \leq D_1 + D_2 \leq 96\sigma\left(\sqrt{n\log\frac{m}{n}} + \sqrt{\log m\log(mn)\log\frac{m}{\log m}}\right).$$

Next we show that the randomized rounding performed in Step 3 incurs small discrepancy. Consider a coordinate $j \in [n]$ that is rounded. Then,

$$\mathbb{E}\left(z(j) - \overline{x}(j)\right) = 0,$$
$$\mathrm{Var}\left(z(j) - \overline{x}(j)\right) \leq \delta,$$

and thus,

$$\Delta_i^2 := \mathrm{Var}\left(\sum_{j=1}^{n} A_{ij}(z(j) - \overline{x}(j))\right) \leq ||A_i||^2\delta.$$

Therefore, for $i \in [m]$, by Chernoff bound,

$$\mathsf{Pr}\left(|\sum_{j=1}^{n} A_{ij}(z(j) - \overline{x}(j))| \geq 4\Delta_i\sqrt{\log m}\right) \leq \frac{2}{m^8}.$$

Hence, by union bound, we get that

$$|A_i(z - \overline{x})| \leq 4\Delta_i\sqrt{\log m} \leq 4\,\|A_i\|$$

for every $i \in [m]$ with probability at least $1 - 1/m^7$. Now, applying Lemma 5, with $\lambda = \sqrt{\log m}$ and using the condition that $\log m \leq n$, we get that $|A_i(z-\overline{x})| \leq 2\sigma\sqrt{n}$ with probability at least $(1-1/m^5)(1-1/m^7) \geq 1-2/m^5$. Thus,

$$|A_i(z - x_0)| \leq |A_i(z-\overline{x})| + |A_i(\overline{x} - x_0)| \leq 192\sigma\left(\sqrt{n\log\frac{m}{n}} + \sqrt{\log m\log(mn)\log\frac{m}{\log m}}\right)\ \forall\ i \in [m]$$

with probability at least $(1-1/m^5)(1-1/(mn)^3)(1-2/m^5) \geq 1 - 4/m^3$.

Finally, we compute the running time of the algorithm. Each call to the Edge-Walk subroutine succeeds with probability 0.1. Hence, the expected number of calls to the Edge-Walk subroutine is at most $10\log n$. Since each call to the Edge-Walk subroutine takes

$$O((m+n)^3\log^3 m\log(nm\log m))$$

time, the expected number of calls is $O(\log n)$ and the number of steps before each call is $O(m+n)$, the total number of steps is at most $O((m+n)^4\log n\log^3 m\log(nm\log m))$. □

4. INFEASIBILITY RADIUS

The upper bound R_1 for the radius in Theorem 1 will follow from the linear discrepancy bound given in Theorem 2. For the lower bound, we show the following result for Gaussian matrices.

LEMMA 10. *For $m \geq 1000n$, let $A \in \mathbb{R}^{m\times n}$ be a matrix whose entries are chosen i.i.d. from the Gaussian distribution $N(0,\sigma^2)$. Let $x_0 := (1/2,\ldots,1/2) \in \mathbb{R}^n$. Then,*

$$\mathsf{Pr}\left(\exists\ x \in \mathbb{Z}^n : A_i(x - x_0) \leq \frac{\sigma}{2}\sqrt{n\log\frac{m}{n}}\ \forall i \in [m]\right) \leq \frac{1}{2^n}.$$

We first show a lower bound on the radius necessary for the random polytope $P(n,m,0,R)$ to contain an integer point with all nonzero coordinates. Lemma 10 will follow from the choice of x_0.

LEMMA 11. *For $m \geq 1000n$, let $A \in \mathbb{R}^{m\times n}$ be a matrix whose entries are chosen i.i.d. from the Gaussian distribution $N(0,\sigma^2)$. Then,*

$$Pr(\exists\ x \in \mathbb{Z}^n : |x_j| > 0\ \forall\ j \in [n], \\ A_i x \leq \sigma\sqrt{n\log\frac{m}{n}}\ \forall i \in [m]\Big) \\ \leq \frac{1}{2^n}.$$

PROOF. For each $r > 0$, we define the set

$$U_r := \mathbb{Z}^n \cap \{x : \|x\| = r, |x_j| > 0\ \forall j \in [n]\}.$$

We will show that with probability at least $1-2^{-n}$ (over the choices of the matrix A), there does not exist $x \in \cup_{r\geq 0} U_r$ satisfying all the m inequalities. We first observe that U_r is non-empty only if $r \geq \sqrt{n}$. Fix $r \geq \sqrt{n}$ and a point $x \in U_r$. Now, for $i \in [m]$, since each A_{ij} is chosen from $N(0,\sigma^2)$, the dot product $A_i x$ is distributed according to the normal distribution $N(0, r^2\sigma^2)$. Let

$$P_x := \mathsf{Pr}\left(A_i x \leq \sigma\sqrt{n\log\frac{m}{n}}\ \forall\ i \in [m]\right),$$
$$P_r := \mathsf{Pr}\left(\exists x \in U_r : A_i x \leq \sigma\sqrt{n\log\frac{m}{n}}\ \forall\ i \in [m]\right).$$

By union bound,

$$P_r \leq \sum_{x\in U_r} P_x \leq |U_r| \max_{x\in U_r} P_x.$$

We will obtain an upper bound on P_x that depends only on r. To bound the size of the set U_r, we observe that every point in U_r is an integer point on the surface of a sphere of radius r centered around the origin and hence is contained in an euclidean ball of radius $r+1$ centered around the origin. Thus, $|U_r|$ can be bounded by the volume of the sphere of radius $r+1 \leq 2r$ centered around the origin:

$$|U_r| \leq \mathrm{vol}\,(2r\mathbb{B}_0) \leq \left(2r\sqrt{\frac{2\pi e}{n}}\right)^n \leq \left(\frac{10r}{\sqrt{n}}\right)^n.$$

Next we bound P_r. We have two cases.

Case 1. Let $r \in \left[\sqrt{n}, \sqrt{n\log(m/n)}\right]$. Since $A_i x$ is distributed according to $N(0, r^2\sigma^2)$, by Lemma 3,

$$\mathsf{Pr}\left(A_i x \leq \sigma\sqrt{n\log\frac{m}{n}}\right) \\ \leq 1 - \frac{1}{\sqrt{2\pi}}\left(\frac{r\sqrt{n\log\frac{m}{n}}}{r^2 + n\log\frac{m}{n}}\right)\cdot\left(\frac{n}{m}\right)^{\frac{n}{2r^2}}.$$

Since each A_{ij} is chosen independently, we have that

$$P_x = \prod_{i=1}^m \mathsf{Pr}\left(A_i x \leq \sigma\sqrt{n\log\frac{m}{n}}\right) \\ < \left(1 - \frac{1}{\sqrt{2\pi}}\left(\frac{r\sqrt{n\log\frac{m}{n}}}{r^2 + n\log\frac{m}{n}}\right)\cdot\left(\frac{n}{m}\right)^{\frac{n}{2r^2}}\right)^m \\ \leq e^{-\frac{1}{\sqrt{2\pi}}\left(\frac{r\sqrt{n\log\frac{m}{n}}}{r^2+n\log\frac{m}{n}}\right)\cdot\left(\frac{n}{m}\right)^{\frac{n}{2r^2}}\cdot m}.$$

Therefore, by union bound, it follows that

$$P_r \leq e^{-\frac{1}{\sqrt{2\pi}}\left(\frac{r\sqrt{n\log\frac{m}{n}}}{r^2+n\log\frac{m}{n}}\right)\cdot\left(\frac{n}{m}\right)^{\frac{n}{2r^2}}\cdot m + n\log\frac{10r}{\sqrt{n}}} \\ \leq e^{-n\log\frac{10r}{\sqrt{n}}} \leq \left(\frac{\sqrt{n}}{10r}\right)^n.$$

Case 2. Let $r > \sqrt{n\log(m/n)}$. Since $A_i x$ is distributed according to $N(0, r^2\sigma^2)$, by Lemma 3, we have that

$$\mathsf{Pr}\left(A_i x \leq \sigma\sqrt{n\log\frac{m}{n}}\right) \leq \frac{1}{r}\sqrt{\frac{1}{2\pi}n\log\frac{m}{n}} \leq \frac{4}{5r}\sqrt{n\log\frac{m}{n}}.$$

The random variables $A_1 x, \ldots, A_m x$ are independent and identically distributed. Therefore,

$$P_x = \prod_{i=1}^m \mathsf{Pr}\left(|A_i x| \leq \sigma\sqrt{n\log\frac{m}{n}}\right) \\ \leq \left(\frac{4}{5r}\sqrt{n\log\frac{m}{n}}\right)^m.$$

Hence, by union bound,

$$P_r \leq e^{-n\left(\frac{m}{n}\log\left(\frac{5r}{4\sqrt{n\log\frac{m}{n}}}\right) - \log\frac{10r}{\sqrt{n}}\right)} \\ \leq e^{-n\left(\frac{m}{2n}\log\left(\frac{5r}{4\sqrt{n\log\frac{m}{n}}}\right)\right)} \\ \leq \left(\frac{4\sqrt{n\log\frac{m}{n}}}{5r}\right)^{\frac{m}{2}}.$$

Finally,

$$\mathsf{Pr}\left(\exists x \in \cup_{r\geq\sqrt{n}} U_r : A_i x \leq \sigma\sqrt{n\log\frac{m}{n}}\ \forall i \in [m]\right) \\ = \sum_{r\geq\sqrt{n}} P_r \\ = \sum_{r\in\left[\sqrt{n}, \sqrt{n\log\frac{m}{n}}\right]} P_r + \sum_{r>\sqrt{n\log\frac{m}{n}}} P_r \\ \leq \frac{1}{10^n}\int_{r=\sqrt{n}}^{\infty}\left(\frac{\sqrt{n}}{r}\right)^n dr \\ + \left(\frac{4}{5}\right)^{\frac{m}{2}}\int_{r=\sqrt{n\log\frac{m}{n}}}^{\infty}\left(\frac{\sqrt{n\log\frac{m}{n}}}{r}\right)^{\frac{m}{2}} dr \\ \leq \frac{1}{10^n}\cdot\frac{\sqrt{n}}{n-1} + \left(\frac{4}{5}\right)^{\frac{m}{2}}\cdot\left(\frac{2\sqrt{n\log\frac{m}{n}}}{m-2}\right) \\ \leq \frac{1}{2^n} \qquad (\text{since } m \geq 1000n).$$

□

PROOF OF LEMMA 10. There exists $x \in \mathbb{Z}^n$ such that

$$A_i(x - x_0) \leq \frac{\sigma}{2}\sqrt{n\log\frac{m}{n}}\ \forall i \in [m]$$

if and only if there exists $x \in \mathbb{Z}^n \cap \{x \in \mathbb{R}^n : |x_j| \geq 1\ \forall\ j \in [n]\}$ such that

$$A_i x \leq \sigma\sqrt{n\log\frac{m}{n}}\ \forall i \in [m].$$

The result follows by Lemma 11. □

5. PROOF OF THRESHOLD RADIUS

We now have all the ingredients needed prove Theorem 1.

PROOF OF THEOREM 1. Let $P = \{x \in \mathbb{R}^n : a_i x \leq b_i \; \forall \, i \in [m]\}$, where each a_i is chosen from a spherically symmetric distribution. Then $\alpha_i = a_i / \|a_i\|$ for $i \in [m]$ is distributed randomly on the unit sphere. A random unit vector α_i can be obtained by drawing each coordinate from the Gaussian distribution $N(0, \sigma^2 = 1/n)$ and normalizing the resulting vector. Thus, we may assume $\alpha_i = A_i / \|A_i\|$ where each coordinate A_{ij} is drawn from the Gaussian distribution $N(0, 1/n)$. Here, we show that the probability that there exists a vector A_i that gets scaled by more than a constant is at most $2me^{-n/96}$.

Taking $\sigma^2 = 1/n$ in Lemma 5, we have

$$\mathsf{Pr}\left(\exists i \in [m] : |\, \|A_i\|^2 - 1| > \frac{1}{2}\right) \leq 2me^{-n}.$$

Hence, with probability at least $1 - 2me^{-n/96}$, we have that $\sqrt{1/2} \leq \|A_i\| \leq \sqrt{3/2}$ for every $i \in [m]$. We now show the upper and lower bounds.

1. Since P contains a ball of radius R_1, it follows that $P \supseteq Q$ where

   $$Q = \{x \in \mathbb{R}^n | \, |\alpha_i(x - x_0)| \leq R_1 \text{ for } i \in [m]\}.$$

   Using Theorem 2 and $\sigma^2 = 1/n$, we know that there exists a randomized algorithm that takes as input A and x_0 and outputs an integer point $x \in \mathbb{Z}^n$ such that for every $i \in [m]$

   $$|A_i(x - x_0)| \leq 192 \left(\sqrt{\log \frac{m}{n}} + \sqrt{\frac{\log m \log (mn)}{n} \log \frac{m}{\log m}}\right).$$

   with probability at least $1 - (4/m^3)$. Thus, with probability at least $1 - (4/m^3) - 2me^{-n}$, we obtain $x \in \mathbb{Z}^n$ satisfying

   $$|\alpha_i(x - x_0)| = \frac{|A_i(x - x_0)|}{\|A_i\|} \leq 384 \left(\sqrt{\log \frac{m}{n}} + \sqrt{\frac{\log m \log (mn)}{n} \log \frac{m}{\log m}}\right)$$

   for every $i \in [m]$. Thus we have an integer point in the polytope Q and hence, an integer point in P.

2. For $x_0 = (1/2, \ldots, 1/2)$, let

   $$P = \{x \in \mathbb{R}^n : A_i(x - x_0) \leq \|A_i\| \sqrt{\frac{1}{6} \log \frac{m}{n}} \; \forall i \in [m]\Big\}.$$

   Then, P contains a ball of radius R_0 centered around x_0 and hence is an instance of the random polytope $P(n, m, x_0, R_0)$. Further, with probability at least $1 - 2me^{-n}$, P is contained in

   $$Q = \left\{x \in \mathbb{R}^n : A_i(x - x_0) \leq \frac{1}{2}\sqrt{\log \frac{m}{n}} \; \forall i \in [m]\right\}.$$

   By Lemma 10, with probability at least $1 - 2^{-n}$, we have that $Q \cap \mathbb{Z}^n = \emptyset$. Thus, with probability at least $1 - 2^{-n} - 2me^{-n}$, we have that $P \cap \mathbb{Z}^n = \emptyset$.

□

6. OPEN QUESTIONS

Propositions 1 and 2 hold for arbitrary constraint matrices describing the polytope. Are these observations useful for solving IP formulations of combinatorial optimization problems for families of instances? A concrete question is whether we can efficiently compute discrepancy or linear discrepancy for a reasonably general family of matrices.

Another open question is the complexity of integer linear optimization on random polytopes as given by our model, with an arbitrary, or even a random objective direction. Our work only addresses integer feasibility.

A natural question that arises there exists a sharp feasibility threshold R^* for the radius, i.e., with high probability, the random polytope $P(n, m, 0, R)$ is integer infeasible (for a nonzero integer point) if $R \leq R^*$ and is integer feasible if $R > R^*$.

Finally, it would be interesting to explore similar phase transition phenomena when the rows of the matrix A are sparse, a setting that can be viewed as a geometric analog of random k-satisfiability.

7. REFERENCES

[1] R. Beier and B. Vöcking. Random knapsack in expected polynomial time. In *Proceedings of the 35th annual ACM symposium on theory of computing*, STOC '03, pages 232–241, 2003.

[2] B. Bollobás. *Random graphs*. Cambridge studies in advanced mathematics. Cambridge University Press, 2001.

[3] A. Broder, A. Frieze, and E. Upfal. On the satisfiability and maximum satisfiability of random 3-cnf formulas. In *Proceedings of the 4th annual ACM-SIAM symposium on discrete algorithms*, SODA '93, pages 322–330, 1993.

[4] M. T. Chao and J. Franco. Probabilistic analysis of two heuristics for the 3-satisfiability problem. *SIAM Journal on Computing*, 15:1106–1118, 1986.

[5] M. T. Chao and J. Franco. Probabilistic analysis of a generalization of the unit-clause literal selection heuristics for the k-satisfiability problem. *Information Sciences*, 51(3):289–314, Aug 1990.

[6] M. Charikar, A. Newman, and A. Nikolov. Tight hardness for minimizing discrepancy. In *Proceedings of the 22nd annual ACM-SIAM symposium on discrete algorithms*, SODA '11, pages 1607–1614, 2011.

[7] A. Charnes, W. W. Cooper, and G. H. Symonds. Cost horizons and certainty equivalents: An approach to stochastic programming of heating oil. *Management Science*, 4(3):pp. 235–263, 1958.

[8] V. Chvátal and B. Reed. Mick gets some (the odds are on his side). In *Proceedings of the 33rd annual symposium on foundations of computer science*, FOCS '92, pages 620–627, 1992.

[9] D. Dadush, C. Peikert, and S. Vempala. Enumerative lattice algorithms in any norm via m-ellipsoid coverings. In *FOCS*, pages 580–589, 2011.

[10] G. Dantzig. On the significance of solving some linear programs with some integer variables. *Econometrica*, 28:30–34, 1960.

[11] E. Friedgut. Sharp thresholds of graph properties and the k-sat problem. *Journal of the American Mathematical Society*, 12:1017–1054, 1998.

[12] M. Furst and R. Kannan. Succinct certificates for almost all subset sum problems. *SIAM J. Comput.*, 18:550–558, June 1989.

[13] R. Hildebrand and M. Köppe. A new lenstra-type algorithm for quasiconvex polynomial integer minimization with complexity $2^{o(n\log n)}$. *Discrete Optimization*, 10(1):69–84, 2013.

[14] R. Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of Operations Research*, 12:415–440, 1987.

[15] R. Karp. Reducibility among combinatorial problems. *Complexity of Computer Computations*, pages 85–103, 1972.

[16] L. Lovász, J. Spencer, and K. Vesztergombi. Discrepancy of set-systems and matrices. *Eur. J. Comb.*, 7:151–160, April 1986.

[17] S. Lovett and R. Meka. Constructive discrepancy minimization by walking on the edges. In *Proceedings of the 53rd annual symposium on foundations of computer science*, FOCS '12, pages 61–67, 2012.

[18] J. Luedtke. An integer programming and decomposition approach to general chance-constrained mathematical programs. In *Integer Programming and Combinatorial Optimization*, pages 271–284. Springer, 2010.

[19] J. Luedtke, S. Ahmed, and G. L. Nemhauser. An integer programming approach for linear programs with probabilistic constraints. *Mathematical Programming*, 122(2):247–272, 2010.

[20] J. Matoušek. An Lp version of the Beck-Fiala conjecture. *Eur. J. Comb.*, 19:175–182, February 1998.

[21] J. Matoušek and J. Spencer. Discrepancy in arithmetic progressions. *American Mathematical Society*, 9(1):195–204, January 1996.

[22] B. L. Miller and H. M. Wagner. Chance constrained programming with joint constraints. *Operations Research*, 13(6):pp. 930–945, 1965.

[23] G. Nemhauser and L. Wolsey. *Integer and Combinatorial Optimization*. Wiley-Interscience, 1999.

[24] A. Nikolov, K. Talwar, and L. Zhang. The geometry of differential privacy: the sparse and approximate cases. In *Proceedings of the 45th annual ACM symposium on theory of computing*, STOC '13, pages 351–360, 2013.

[25] G. Pataki, M. Tural, and E. B. Wong. Basis reduction and the complexity of branch-and-bound. In *Proceedings of the 21st Annual ACM-SIAM symposium on Discrete Algorithms*, SODA '10, pages 1254–1261, 2010.

[26] A. Prékopa. On probabilistic constrained programming. In *Proceedings of the Princeton symposium on mathematical programming*, pages 113–138. Princeton University Press Princeton, NJ, 1970.

[27] A. Prékopa. Probabilistic programming. *Handbooks in operations research and management science*, 10:267–351, 2003.

[28] A. Ruszczyński. Probabilistic programming with discrete distributions and precedence constrained knapsack polyhedra. *Mathematical Programming*, 93(2):195–215, 2002.

[29] A. Schrijver. *Theory of Linear and Integer Programming*. John Wiley & sons, 1998.

[30] J. Spencer. Six standard deviations suffice. *Trans. Amer. Math. Soc.*, 289:679–706, 1985.

[31] J. Spencer. Ten lectures on the probabilistic method. *SBMS-NSF, SIAM*, 1987.

[32] H. Yanagisawa and T. Osogami. Improved integer programming approaches for chance-constrained stochastic programming. In *Proceedings of the 23rd international joint conference on Artificial Intelligence*, pages 2938–2944, 2013.